The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

Subject:
Multiple Vulnerabilities for CA Anti-Virus Engine (CA20091008-01)

Overview:
CA's support is alerting customers to multiple security risks associated with CA Anti-Virus Engine. Vulnerabilities exist in the arclib component that can allow a remote attacker to cause a denial of service, or to cause heap corruption and potentially further compromise a system. CA has issued fixes to address the vulnerabilities.

The first vulnerability, CVE-2009-3587, is due to improper handling of a specially crafted RAR archive file by the CA Anti-Virus engine arclib component. An attacker can create a malformed RAR archive file that results in heap corruption and allows the attacker to cause a denial of service or possibly further compromise the system.

The second vulnerability, CVE-2009-3588, is due to improper handling of a specially crafted RAR archive file by the CA Anti-Virus engine arclib component. An attacker can create a malformed RAR archive file that results in stack corruption and allows the attacker to cause a denial of service.

Systems Affected:
Windows
UNIX
Linux
Solaris
Mac OS X
Netware

Risk:
Medium

Affected Products:
CA Anti-Virus for the Enterprise (formerly eTrust Antivirus) 7.1
CA Anti-Virus for the Enterprise (formerly eTrust Antivirus) r8
CA Anti-Virus for the Enterprise (formerly eTrust Antivirus) r8.1
CA Anti-Virus 2007 (v8)
CA Anti-Virus 2008
CA Anti-Virus 2009
CA Anti-Virus Plus 2009
eTrust EZ Antivirus r7.1
CA Internet Security Suite 2007 (v3)
CA Internet Security Suite 2008
CA Internet Security Suite Plus 2008
CA Internet Security Suite Plus 2009
CA Threat Manager for the Enterprise (formerly eTrust Integrated Threat Management) r8
CA Threat Manager for the Enterprise (formerly eTrust Integrated Threat Management) 8.1
CA Threat Manager Total Defense
CA Gateway Security r8.1
CA Protection Suites r2
CA Protection Suites r3
CA Protection Suites r3.1

CA Secure Content Manager (formerly eTrust Secure Content Manager) 1.1
CA Secure Content Manager (formerly eTrust Secure Content Manager) 8.0
CA Network and Systems Management (NSM) (formerly Unicenter Network and Systems Management) r3.0
CA Network and Systems Management (NSM) (formerly Unicenter Network and Systems Management) r3.1
CA Network and Systems Management (NSM) (formerly Unicenter Network and Systems Management) r11
CA Network and Systems Management (NSM) (formerly Unicenter Network and Systems Management) r11.1
CA ARCserve Backup r11.5 on Windows
CA ARCserve Backup r12 on Windows
CA ARCserve Backup r12.0 SP1 on Windows
CA ARCserve Backup r12.0 SP 2 on Windows
CA ARCserve Backup r12.5 on Windows
CA ARCserve Backup r11.1 Linux
CA ARCserve Backup r11.5 Linux
CA ARCserve for Windows Client Agent
CA ARCserve for Windows Server component
CA eTrust Intrusion Detection 2.0 SP1
CA eTrust Intrusion Detection 3.0
CA eTrust Intrusion Detection 3.0 SP1
CA Common Services (CCS) r3.1
CA Common Services (CCS) r11
CA Common Services (CCS) r11.1
CA Anti-Virus SDK (formerly eTrust Anti-Virus SDK)
CA Anti-Virus Gateway (formerly eTrust Antivirus Gateway) 7.1

Non-Affected Products:
CA Anti-Virus engine with arclib version 8.1.4.0 or later installed

Solution:
CA released arclib 8.1.4.0 on August 12 2009. If your product is configured for automatic updates, you should already be protected, and you need to take no action. If your product is not configured for automatic updates, then you simply need to run the update utility included with your product.
CA Network and Systems Management (NSM) (formerly Unicenter Network and Systems Management) r3.0: apply fix # RO11964.
CA Network and Systems Management (NSM) (formerly Unicenter Network and Systems Management) r3.1: apply fix # RO11964.
CA Network and Systems Management (NSM) (formerly Unicenter Network and Systems Management) r11: apply fix # RO11964.
CA Network and Systems Management (NSM) (formerly Unicenter Network and Systems Management) r11.1: apply fix # RO11964.
CA Common Services (CCS) r3.1: apply fix # RO11954.
CA Anti-Virus for the Enterprise (formerly eTrust Antivirus) 7.1 32bit: apply fix # RO10663.
CA Anti-Virus for the Enterprise (formerly eTrust Antivirus) 7.1 IA64: apply fix # RO10664.
CA Anti-Virus for the Enterprise (formerly eTrust Antivirus) 7.1 AMD64: apply fix # RO10665.
CA Secure Content Manager (formerly eTrust Secure Content Manager) r1.1: apply fix # RO10999.
CA Secure Content Manager (formerly eTrust Secure Content Manager) r8.0: apply fix # RO10999.
CA Anti-Virus Gateway (formerly eTrust Antivirus Gateway) 7.1: apply fix # RO11000.
CA Gateway Security r8.1: RO10999.
CA ARCserve for Windows Server component installed on a 64 bit machine: apply fixes # RO10663 and RO10664 (IA64) or RO10665 (AMD64).
CA ARCserve for Windows Server component installed on a 32 bit machine: apply fix # RO10663.

CA ARCserve for Windows Client Agent installed on a 64 bit machine: apply fix # RO10664 (IA64) or RO10665 (AMD64).
CA ARCserve for Windows Client Agent installed on a 32 bit machine: apply fix # RO10663.
CA ARCserve for Linux Server r11.5: apply fix # RO10729.
CA ARCserve for Linux

Workaround:
Do not open email attachments or download files from untrusted sources.

REFERENCES:

CA
https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=218878

CVE
CVE-2009-3587 - CA Anti-Virus RAR archive heap corruption
CVE-2009-3588 - CA Anti-Virus RAR archive stack corruption